PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A1	(11) International Publication Number: WO 97/12460
		(43) International Publication Date: 3 April 1997 (03.04.97)

(21) International Application Number: PCT/US96/14159

(22) International Filing Date: 23 August 1996 (23.08.96)

(30) Priority Data:
08/528,841 15 September 1995 (15.09.95) US

(71) Applicant: DOCUMENT AUTHENTICATION SYSTEMS, INC. [US/US]; 1500 Three Lincoln Centre, 5430 LBJ Freeway, Dallas, TX 75240-2387 (US).

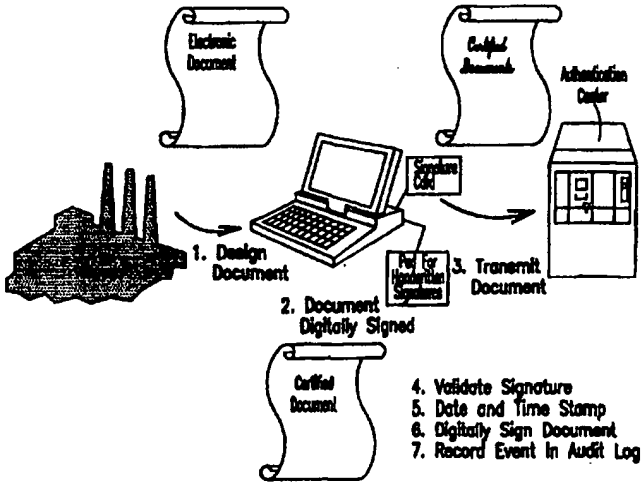
(72) Inventors: BISBEE, Stephen, F.; 738 Broadwater Way, Gibson Island, MD 21506 (US). MOSKOWITZ, Jack, J.; 4632 Autumn Woods Way, Ellicott City, MD 21043 (US). SHEEHAN, Edward, R.; 1924 Pine Knob Road, Sykesville, MD 21784 (US). TROTTER, Douglas, H.; 4332 N. Charles Street, Baltimore, MD 21218 (US). WHITE, Michael, W.; 1913 Midland Road, Baltimore, MD 21222 (US).

(74) Agents: SAVAGE, Michael, G. et al.; Burns, Doane, Swecker & Mathis L.L.P., P.O. Box 1404, Alexandria, VA 22313-1404 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DOCUMENT AUTHENTICATION SYSTEM AND METHOD



(57) Abstract

Methods and apparatus are provided that implement digital signing(2 and 3) and/or encryption for the electronic transmission, (3) storage, and retrieval of authenticated documents and that enable the establishment of the identity of the originator of an electronic document and of the integrity of the information contained in such a document (1). Together these provide irrevocable proof of authenticity of the document. The methods and apparatus make it possible to provide "paper-less" commercial transactions, such as real-estate transactions and the financial transactions secured by real estate. A Certification Authority provides tools for initializing and managing the cryptographic material required to sign and seal electronic documents. An Authentication Center provides "third party" verification that a document is executed and transmitted by the document's originator. The methods and apparatus eliminate the need for "hard copies" of original documents as well as hard-copy storage. Retrieval of an authenticated document from the Authentication Center may be done by any number of authorized parties at any time by on-line capability.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

DOCUMENT AUTHENTICATION SYSTEM AND METHOD

BACKGROUND

Applicant's invention relates to systems and methods for providing a verifiable chain of evidence and security for the transfer and retrieval of documents in digital formats.

Paper documents are the traditional evidence of the communications and agreements between parties in commercial and other transactions. Financial and real-estate transactions are protected by paper-based controls. Signatures and safety paper (such as pre-printed checks) facilitate detection of unauthorized alterations of the information of commercial transactions. Important documents may also be provided with "third man" controls, by the witnessing of signatures and by the seal and acknowledgement of a Notary Public.

The methods of commerce, however, have changed dramatically and continue to evolve. This is most evident in the replacement of paper-based communications with electronic communications. The "due care" controls used with paper-based communications do not exist in routine electronic transactions. Standard electronic communication over open systems does not have the same ability to provide authentication, privacy, and integrity of the communicated information. By "authentication" is meant verification of the identity of the signatory of a document; by "privacy" is meant protection of the information in a document from unauthorized eyes; and by "integrity" is meant the ability to detect any alteration of the contents of a document.

When communication is by electronically reproduced messages such as e-mail, facsimile machine, imaging, electronic data interchange or electronic fund transfer, there no longer exists a signature or seal to authenticate the identity of the transferor. The traditional legally accepted methods of verifying the identity of a document's originator, such as physical presence or appearance, an ink signature, personal witness or Notary Public acknowledgement, are not possible.

The continued evolution of computer and telecommunications technology has regretfully been accompanied by the invention of more and more sophisticated ways to intercept and alter information electronically transmitted, including the widespread phenomenon of remote intrusion of computer systems through telecommunication links.

Some approaches to providing secure electronic commerce technology by applying cryptography give the user a verification mechanism for the authenticity or privacy of the transmission that is controlled by the user and does not include the element of non-repudiation. In some cases the use of encryption for privacy could aid in the detection of document alterations, advancing the goal of integrity. This is not generally the case, however, and additional mechanisms may be required for providing integrity. At present, no distributed electronic document authentication system exists that can provide authentication, as with written or printed instruments, in a manner that cannot be repudiated. No commercial system provides electronic document verification based on a digital signature that cannot be repudiated, although some attempts have been described. See, e.g., D. Chaum, "Achieving Electronic Privacy", Scientific American, vol. 247, no. 8, pp. 96-101 (Aug. 1992); C.R. Merrill, "Cryptography for Commerce Beyond Clipper", The Data Law Report, vol. 2, no. 2, pp. 1, 4-11 (Sep. 1994). Since DES, no governmental organization or other standards-setting body has been willing or able to set standards (i.e., as to cryptographic strength, process, etc.) acceptable for general commercial use. The techniques described in this application are synergistic and of sufficient assurance to be on par with the security needed to support a typical business transaction.

Applicant's document authentication system (DAS) provides the needed security and protection of electronic transmissions. Most important to commercial and financial institutions, Applicant's DAS assumes the risk and responsibility of a document's authenticity. Applicant's DAS utilizes an asymmetric cryptosystem,

known as a public-key system, to help ensure that the party originating a document is electronically identifiable as such.

Various aspects of public-key cryptographic (PKC) systems are described in the literature, including R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM vol. 21, pp. 120-126 (Feb. 1978); M.E. Hellman, "The Mathematics of Public-Key Cryptography", Scientific American, vol. 234, no. 8, pp. 146-152, 154-157 (Aug. 1979); and W. Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, vol. 76, pp. 560-577 (May 1988). Popular PKC systems make use of the fact that finding large prime numbers is computationally easy but factoring the products of two large prime numbers is computationally difficult. A PKC system is an asymmetric encryption system, meaning that it employs two keys, one for encryption and one for decryption. Asymmetric systems adhere to the principle that knowledge of one key (the public key) does not permit derivation of the second key (the private key). Thus, PKC permits the user's public key to be publicly posted (e.g., in a directory or on a bulletin board), without compromising the user's private key. This public key concept simplifies the key distribution process.

Besides the PKC method, another encryption method is the symmetric algorithm. An example of this is the Data Encryption Standard (DES), which is described in Data Encryption Standard, Federal Information Processing Standards Publication 46 (1977) ("FIPS PUB 46", republished as FIPS PUB 46-1 (1988)) and DES Modes of Operation, FIPS PUB 81 (1980) that are available from the U.S. Department of Commerce. See also W. Diffie et al., Privacy and Authentication: An Introduction to Cryptography , Proc. IEEE vol. 67, pp. 397-427 (Mar. 1979). In general, a symmetric cryptographic system is a set of instructions, implemented in either hardware, software or both that can convert plaintext (the unencrypted information) to ciphertext, or *vice versa*, in a variety of

ways, using a specific key that is known to the users but is kept secret from others.

For either a symmetric or PKC system, the security of a message is dependent to a great extent on the length of the key, as described in C.E. Shannon, "Communication Theory of Secrecy Systems", Bell Sys. Tech. J. vol. 28, pp. 656-715 (Oct. 1949).

SUMMARY

These and other objects and advantages are provided by the DAS which comprises the means to identify the originator of the electronic document, to provide irrevocable proof of the integrity of the transmission of an electronic document and the means to prevent the originator of the document from denying the document's originator, i.e., non-repudiation.

In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes.

The signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and encrypting the message digest with a secret cryptographic key of the Transfer Agent. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest.

The method may further comprise the step of applying a date stamp and a time stamp to the electronic document. The date and time stamps may be applied either before or after validation of the digital signature and electronic document using the certificate. Also, the method may further comprise the step of signing the electronic document with a second digital signature.

In another aspect of the invention, an apparatus for authenticating an electronic document comprises means for signing the electronic document with a digital signature of a Transfer Agent; means for appending a certificate to the electronic document; and means for validating the digital signature and certificate. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes.

The signing means may comprise means for applying a hash function to the electronic document to determine a message digest and means for encrypting the message digest with the Transfer Agent's secret cryptographic key. The validating means may then comprise means for decrypting the message digest with a public cryptographic key of the Transfer Agent, means for applying the hash function to the electronic document to determine a second message digest, and means for comparing the decrypted message digest to the second message digest.

The apparatus may further comprise means for applying a date stamp and a time stamp to the electronic document. The date and time stamps may be applied either before or after the digital signature and electronic document have been validated using the certificate. Also, the apparatus may further comprise means for signing the electronic document with a second digital signature.

In another aspect of Applicant's invention, an authentication system for the electronic transmission of documents comprises a device for digitally encrypting a document; a device for certifying the identity of the document transferor; a device for generating a public key and a private key; a device for signing the document with a digital signature; a device for verifiably transmitting the electronic

document; and a device for authenticating transmission of the electronic document; whereby the system ensures the integrity of the transmitted document and the non-repudiation of the transmitted document by the document transferor.

In another aspect of the invention, an electronic document storage and retrieval system comprises a device for securely storing of digitally encrypted electronic documents; a device for authenticating of electronic documents retrieved from storage; and a device for verifying the authority of the party requesting the authenticated electronic document; whereby the system ensures the authenticity of the electronic document stored within the system and the transfer of the electronic document to authorized parties.

In another aspect of the invention, a method of authenticating electronically transmitted documents comprises the steps of digitally encrypting a document; certifying the identity of the document transferor; generating a public key and a private key; signing the document with a digital signature; verifiably transmitting the electronic document; and authenticating transmission of the electronic document; whereby the integrity of the transmitted document and the non-repudiation of the transmitted document by the document transferor is ensured.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of Applicant's invention will become apparent by reading this description in conjunction with the drawings in which:

FIG. 1 is a block diagram of the liability allocation for authentication in the DAS;

FIG. 2 summarizes the functions of the DAS relating to document transmission authorization and protection;

FIG. 3 is a simple diagram of the DAS architecture;

FIG. 4 is a block diagram of the functional interrelationship between a Transfer Agent and an Authentication Center;

FIG. 5 is a block diagram of DAS control functions;

FIGs. 6a, 6b are diagrams illustrating application of the DAS in the mortgage finance industry with a title company/closing agent for a loan as a Transfer Agent;

FIG. 7 illustrates the document certification process more generally;

FIG. 8 illustrates generation of a digital signature;

FIG. 9 illustrates digitally signing a document and validation of the digital signature;

FIG. 10 illustrates the format of a certificate employed by a user or the Certification Authority;

FIG. 11 illustrates validation of certificates; and

FIG. 12 illustrates generation of certificates.

DETAILED DESCRIPTION

Applicant's invention can be implemented utilizing commercially available computer systems and technology to create an integrated closed system for authentication of electronic documents.

Referring to FIG. 1, which is a block diagram of the liability allocation for authentication in Applicant's DAS, the DAS uses a Certification Authority framework by which public/private keys, that are utilized to encrypt/decrypt and/or digitally sign a document, are delivered to a document's originator by an established, auditable means. Certificates and certification frameworks are described in the above-cited publication by C.R. Merrill and in ITU-T Recommendation X.509 (1993)|ISO/IEC 9594-8:1995 Information Technology Open Systems Interconnection The Directory: Authentication Framework (including all amendments), which are expressly incorporated here by reference. The infrastructure and certificate definitions used in this application are based on these documents.

As described below, the public/private key is advantageously delivered in the form of a token such as an electronic circuit card conforming to the standards of the PC Memory Card Interface Association (a PCMCIA card or PC Card) for use in the originator's computer. In general a token is a portable transfer device that is used for transporting keys, or parts of keys. It will be understood that PC Cards are just one form of delivery mechanism for public/private keys for Applicant's DAS; other kinds of tokens may also be used, such as floppy diskettes and Smart Cards. To ensure reliable delivery a service such as the bonded courier services commonly used to ferry securities between parties could be used to deliver the media to the document originator.

Advantageously, many commercially available tokens that embody on-board cryptography generate the public/private key pairs on the cards, and the private keys never leave the cards unencrypted. The public keys are exported to the Certification Authority for inclusion, with the identity of the intended recipient and appropriate user attributes among other things, into a "certificate". Principal components of the DAS system assurance are the correct operation of the Certification Authority framework, the tight binding of user identity and attributes to the public key in the certificate, and the reliable delivery of the PC Card to the authorized recipient.

In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered separate from the originator's card. Any subsequent transmitter of the document who is required to digitally sign or encrypt the document would similarly be provided with a respective card and personal identification information.

In FIG. 1, a document's originator and any subsequent transmitter are called a Transfer Agent, and it will be appreciated that a Transfer Agent is identified to the DAS by its possession and use of a valid certificate and a valid PIN. In issuing the key and PIN to the Transfer Agent, the DAS advantageously records one or more attributes, or characteristics, of the Transfer Agent in association with the key and PIN. For example, the Transfer Agent may be authorized to conduct only certain types of transactions and/or transactions having less than a predetermined value.

Issuance by the Certification Authority of a digitally signed certificate ensures the verifiability of the identity of each transmitter of a digitally signed or encrypted document. The Certification Authority also retains the ability to revoke a public/private key, or to reissue a public/private key, from a remote location electronically. The Certification Authority can also support privilege management in accordance with the policy set for the system. For example, the Certification Authority can set financial or other limits on the authority granted to the Transfer Agent by conveying those authorizations or restrictions as certificate attributes. These attributes can be retrieved from the certificate and enforced by other elements in the system.

In an important aspect of Applicant's invention, the DAS is a system for authenticating a document by applying digital signature encryption technology for the electronic transmission of the document. As used here, "authentication" is the corroboration and verification of the identity of the party which executed, sealed, or transmitted the original document and verification that the encrypted document received is the document sent by that party. The DAS uses an Authentication Center to provide an audit or evidence trail, for applications that require this capability, from the original execution of the executed or encrypted or sealed document through all subsequent transmissions.

The Certification Authority would use a physically secure facility that is a "trusted center" having twenty-four-hour security, an alarm system, and "vaulted" construction. In view of its importance, a facility would advantageously include two-person controls, with no single person having access to key generating or key management systems. All personnel connected with the operations of cryptographic key management and transmission of electronic documents would have their trustworthiness evaluated in the surest ways possible, e.g., personal interviews, background checks, polygraphs, etc. Moreover, the Certification Authority management would implement procedures that prevent single-point failures, requiring collaboration for compromise to take place. In this way, one individual would be prevented from obtaining complete access to key generation and to key management.

Another aspect of Applicant's DAS authentication that is in contrast to prior systems is the utilization of an integrity block and a date and time "stamp" on each transmitted document. Suitable time and date stamps are those provided by systems described in U.S. Patents No. 5,136,646 and No. 5,136,647 to Stuart A. Haber and W.S. Stornetta, Jr., both of which are expressly incorporated here by reference, and commercially available from Surety Technologies, Inc. The integrity block, i.e., the digital signature, and the date and time stamp, which are applied by the Authentication Center, eliminate the possibility of unauthorized alteration or tampering with a document by the signatories subsequent to its original execution or sealing. The Authentication Center's integrity block for a document received from a Transfer Agent is generated using any of several known digital hashing algorithms. This integrity block ensures that the document cannot be altered without detection. In addition, use of the digital signing algorithm by the Authentication Center can advantageously provide for non-repudiation, i.e., precluding the originator from disavowing the document. Applicant's combination of the integrity block, date and time stamp, and audit provide notice and evidence

of any attempt at alteration or substitution, even by a document's originator when the alteration is attempted after origination.

In accordance with Applicant's invention, each transaction and its documents are authenticated by transmission to the Authentication Center from the Transfer Agent's terminal. As described below, the Transfer Agent provides the document in digital form, such as the output of a conventional word processor, to the Transfer Agent's PCMCIA card. As an option, a device for digitizing a hand-written signature may also be provided and the digitized signature may be added to the digital document. The digital document is digitally signed and/or encrypted by the DAS PCMCIA card, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (e.g., by modem or computer network). Other ways of communicating the digitally signed or encrypted documents might be used (for example, dispatching a diskette containing the document), but the great advantage of electronic communication is speed.

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. The combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Applicant's invention provides for authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity.

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication

Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication as described above and stores the authenticated documents for transmission to and on behalf of authorized parties whose identities and policies are similarly authenticated by the Authentication Center. Authorization for access may be restricted to the level of a single document or group of documents.

In accordance with Applicant's invention, the DAS verifies and ensures that documents that have been transmitted, stored, or retrieved have not been accidentally or intentionally modified. The DAS can verify at any stage and at any time that a document is exactly, to the last digital bit, the document which was executed and transmitted by the originator and that the document has not been altered or impaired in any manner. This element of integrity combined with a digital signature and a date and time stamp enable the DAS to ensure that a document is not a fabrication, forgery, impersonation, or unauthorized replacement of a document originally executed or sealed by the document's originator.

Since originators of documents to be signed and/or encrypted, such as loan and mortgage documents, commercial paper and other securities, property deeds and leases, etc., should be able to execute their transactions from a variety of locations, the DAS moves the heart of the cryptographic process to a PCMCIA cryptographic card entrusted to a respective authorized Transfer Agent. This permits individual utilization of any DAS enabled computer in any location that is networked or connected with the Authentication Center. As described above, the cryptographic cards and certificates are issued and monitored by the Certification Authority. Certificates may be further controlled through the inclusion of an "expiration period" field, which enables the periodic replacement if desired of the Transfer Agent certificates. It will be appreciated that certificates in accordance

with X.509 include a plurality of such fields, but only those fields important to understanding the operation of the invention are described here.

FIG. 2 summarizes the functions of the DAS relating to document transmission authorization and protection. In the left column are the functions of a Transfer Agent's PC Card; in the center column are other functions carried out by the Transfer Agent's transmission device; and in the right column are functions of the DAS. FIG. 3 is a diagram illustrating interconnections among three Transfer Agent terminals and a server subsystem and backup subsystem in the Authentication Center in the DAS architecture. FIG. 4 is a block diagram of the functional interrelationship between a Transfer Agent and the Authentication Center.

The cryptographic card includes components, such as a microprocessor and electronic memory devices, for carrying out the steps of a PKC algorithm as well as a symmetric encryption algorithm such as DES. Also, the card should be tamper-proof, which can be assured by designing it to delete critical keys and/or algorithms upon any attempted penetration or alteration. The National Institute of Standards and Technology has been chartered to certify the authentication implementation of the cryptographic card suppliers that may be used by the DAS.

In accordance with Applicant's invention, each transaction and its documents are authenticated using a public key contained in the Transfer Agent's certificate. Privacy, signature, and/or integrity devices and software are commercially available from a number of sources, including RSA Data Security, Inc.; Public Key Partners; Surety Technologies, Inc.; Ascom Tech AG, Switzerland; National Semiconductor; Northern Telecom Ltd.; and Spyrus.

The Authentication Center makes use of its own secret key to sign again the transaction in a manner that cannot be repudiated. The combination of the Transfer Agent's and Authentication Center's signatures (in conjunction with the physically protected audit trail) can be used at a future date to prove conclusively

that an agent, employee, or firm (the Transfer Agent) initiated a specific transaction. In addition, a Notary Public support function is available for implementation as described below.

Employee or agent sign-on at the Transfer Agent's terminal is protected by the personal identification information and the cryptographic features of the cryptographic card held by that Transfer Agent. The combination of these controls uniquely identifies the agent or employee, thereby enabling DAS. In addition, agent or employee authorization and attribute information may be stored in the certificates or PCMCIA card memory in protected or sealed form as described above. The DAS uses this information in conjunction with the PIN to set privilege, access, volume and fund amount limits.

The DAS provides a distributed validation capability using a "signature" that cannot be repudiated. The strategy uses PKC to reduce the key management overhead and to provide a digital signature that cannot be repudiated for all documents and transactions. Encryption is used to provide confidentiality protection of the PIN and other transaction details as described above. These control functions of the DAS are summarized in FIG. 5.

Additionally, the DAS is compatible with the full range of modern distributed, and client/server transactional based applications. It operates effectively in LAN, WAN, and dial-up networks. The DAS preferably utilizes modern database tools, and thus the server can advantageously utilize relational technology with a SQL interface (e.g., SYBASE).

The DAS can utilize a variety of technology based tools that may be outlined as follows. The security architecture may allocate liability on a basis that cannot be repudiated by using approved industry standards. In particular ANSI X9.9 and X9.19, which are incorporated here by reference, may be used for authentication. The DES may be used for encryption of the documents, and triple encryption may be used to protect key encrypting. The session key management

option of ANSI X9.24, Financial Institution Retail Key Management, which is incorporated here by reference, may be used in conformance with the security architecture.

In one aspect of Applicant's invention, documents, transactions and other information may be protected by using ANSI standard cryptographic techniques. PINs may be encrypted using DES; selected message elements may be authenticated using the methods defined in ANSI X9.9, Financial Institution Message Authentication (Wholesale); and cryptographic key management may conform to ANSI X9.17, Financial Institution Key Management (Wholesale), which is incorporated here by reference. The technology specified in these standards protects the integrity of transactions against fraud and manipulation.

As illustrated in FIG. 4, the originator of an electronic document or other Transfer Agent may implement the DAS with a typical 486 desktop or laptop computer having the DAS encryption subsystem (PCMCIA card) installed and optionally an electronic digital signature pad for hand-signed "execution" of the document. It is not required for the function of the DAS to have a hand-signed instrument since a digital signature on the document is sufficient. However, at this time, a typical party in loan or other commercial transactions requires the comfort of receiving laser-printed copies of documents which have been executed by hand. Other components and software typically provided in the Transfer Agent terminal are a communication subsystem for handling transmission of encrypted or digitally signed documents to the Authentication Center by a modem telephone line or other suitable communication link, a PCMCIA card interface, a message handler, input/output interface, and multimessage input application.

The Authentication Center is advantageously organized as a server subsystem, a crypto backup subsystem, and storage. As part of the server subsystem, which may be implemented with a 486 computer running under a UNIX-type operating system, a terminal communication subsystem includes a

multiport controller (see also FIG. 3) that handles communications with the Transfer Agent terminals. Also provided in the server subsystem are a cryptographic key management subsystem, a backup subsystem, a relational database management system, input/output (I/O), system administration, and audit subsystem. A PCMCIA Card and backup communication subsystem interfaces with the backup subsystem mentioned above that may be implemented as a 486 computer running under a DOS-type operating system. A storage communication subsystem interfaces with the document storage device or devices mentioned above.

The DAS also would permit a "Notary Public" type of secondary support function. This would permit a third party present at the document's execution to also have a cryptographic card which would "seal" the transaction for further verification that the parties executing or sealing the document to be signed were in fact the proper parties. This additional notary function is not required, but would assist in the further authentication of the identities of the parties.

FIGs. 6a, 6b are diagrams illustrating a typical application of the DAS in the mortgage finance industry with a title company/closing agent for the loan as a Transfer Agent. In step 1, the Certification Authority completes code generation and issues PCMCIA cards to authorized parties for transferring documents and establishing legal evidence trails. The parties, who would generally not be individuals but commercial and financial institutions such as a BANK/Mortgage Co. and a Title Co./Closing Agent, would be equipped to transmit and receive documents electronically. In step 2, a Bank/Mortgage Co. loads and electronically transmits loan documents to the Authentication Center, which forwards them to a Title Co./Closing Agent after adding integrity blocks and date and time stamps. In step 3, the Authentication Center transmits the authenticated loan documents to the Title Co./Closing Agent.

In step 4, the Title Co./Closing Agent has the documents executed by digitized autograph signature by a Homebuyer/Homeowner. In step 5, the Title Co./Closing Agent provides Homeowner/Homebuyer with "hard copies" of the signed documents. In step 6, the Title Co./Closing Agent transmits the documents to the Authentication Center, which adds the integrity blocks and dates and time stamps the executed documents, forwards the documents to the Bank/Mortgage Co., and stores the documents. Whenever the Bank/Mortgage Co. needs copies of the authentic documents, they can be retrieved on-line from Authentication Center storage.

In step 7, the Bank/Mortgage Co. directs that the authentic documents be transferred by the Authentication Authority to a secondary-market Mortgage Bank/Investor. In step 8, whenever the Investor needs authentic documents, they can be retrieved on-line from the Authentication Center.

FIG. 7 further illustrates an example of Applicant's document certification process. In the first step, an electronic document is designed, or drafted, that reflects the agreement of parties, such as a manufacturing operation depicted by the factory in FIG. 7. The electronic document is provided to a Transfer Agent's terminal, which is illustrates as a portable computer having an authorized PC Card and, optionally, a stylus pad for capturing hand-written signatures. A typical configuration for a Transfer Agent's terminal is at least the computational equivalent of a 386 desktop or laptop computer, with high resolution graphics, a PC Card reader, and a stylus pad for capturing hand-written signatures. As shown in FIG. 7, the electronic document, which may be created locally or remotely, is displayed on this terminal.

In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document. After all parties have signed the document, the Transfer Agent certifies the completion of the

document's execution by invoking his or her digital signature and appending his or her certificate, using the PC Card.

If an original paper document were desired, the electronic document would be printed first. The paper document would then be placed on the stylus pad and the terminal's cursor positioned to the corresponding place in the electronic document. This permits the capture and transfer of hand-written signatures during the actual signing of the paper document. The electronic version is then an exact duplicate of the paper document.

After local certification, the Transfer Agent transmits the electronic document to the Authentication Center in the third step of the process. The Authentication Center preferably includes a high-volume utility server computer, having substantial storage capacity and backup capability, and is a secure and highly assured facility. The Authentication Center contains a separate digital signature capability, one or more PC Cards, and an accurate time base.

When an electronic document is received, the authenticity and rights of the Transfer Agent are validated by the Authentication Center (step 4). If authenticated, the electronic document is time- and date-stamped (step 5), digitally signed (step 6), journaled (step 7), and stored by the Authentication Center. Certified copies of the electronic document may then be distributed according to instructions from an appropriate party, such as the holder of a beneficial interest (owner) designated by the document.

The Authentication Center maintains the electronic document and a log, or history, of all transactions, such as requests for copies, etc., related to it. It will be appreciated that the log is useful for many management functions that contribute to the usefulness of the system. For example, the log facilitates identifying subsequent electronic submissions related to a transaction and contributes to liability limitation for the Authentication Center. Also, the log is useful as evidence of the document's chain of custody.

The Authentication Center also controls access to the document in accordance with authorization instructions provided by the owner of the document. Such authorization instructions would be updated or revised in conformance with changes (e.g., assignments) in the document's ownership.

FIG. 8 illustrates the process of digitally signing an electronic document, depicted more generally as an "information object", by application of a hash function. In general, a hash function is a truly one-way cryptographic function that is computed over the length of the information object to be protected. The hash function produces a "message digest" in a way such that no two different information objects produce the same message digest. Since a different message digest is produced if even one bit of the information object is changed, the hash function is a strong integrity check.

In accordance with the invention, the message digest is encrypted using the signatory's secret key, thereby producing the signatory's digital signature. The combination of hashing and encryption in this way insures the system's integrity (i.e., the ability to detect modification) and attribution capability (i.e., ability to identify a signatory, or responsible party). The digital signature (the encrypted message digest) is appended to the readable information object (see steps 2 and 6 depicted in FIG. 7).

Of the many different hash functions that are known, it is currently believed that those designated MD4 and MD5, which are embodied in circuits commercially available from vendors identified above, and the U.S. government's published secure hash algorithm are suitably robust for use in Applicant's DAS. Of course, other hash functions can be expected to become available as time passes.

The steps of digitally signing an electronic document (steps 2 and 6 depicted in FIG. 7) and validating the digital signatures (step 4 in FIG. 7) are further illustrated in FIG. 9. The electronic document has appended to it one or

more digital signatures, which are created by using a signature algorithm and the secret key(s) of the signatory(s) as described in connection with FIG. 8, and the certificate(s) of the signatory(s). As described above, each such certificate conveys the identity of the signatory, the signatory's public signature/verification key, predetermined collateral information about the signatory, and the digitally signed message digest of the certificate. The format of these pertinent parts of such a certificate in accordance with the X.509 Recommendation that would be employed by a user or the Certification Authority is illustrated in FIG. 10.

The signature validation step, which would normally but not necessarily be carried out by the Authentication Center, comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document.

As shown in FIG. 11, a certificate of a user (Transfer Agent) or even of a Certification Authority is preferably digitally signed in substantially the same way that electronic documents are digitally signed, except that such a certificate is signed by authorities specifically empowered to create certificates. Validation of a document's digital signatures includes validation of the public signatures of all Certification Authorities in a path between the signatory and a Root Authority, which is the most superior Certification Authority. The signatures of these Certification Authorities are loaded in the signatory's PC Card and appended to documents prepared with that PC Card.

As illustrated by FIG. 12, the path from the signatory to the Root Authority may be considered part of an authentication tree. The signatory's (user's) certificate is digitally signed by a Certification Authority whose own certificate (the CA Certificate) is signed by the Root Certification Authority. Since there is likely to be a plurality of Certification Authorities located on different branches of the authentication tree, it is only necessary to retrieve all Certification Authority certificates along both branches until a common node is encountered, in order to authenticate a digital signature for an entity on a different branch of an authentication tree, and to verify the authenticities of the certificates up to the common node.

It will be noted that the present description and drawings are illustrative only and that one of ordinary skill in the art would recognize that various modifications could be made without departing from the spirit or scope of the present invention which is to be limited only by the following claims.

WHAT IS CLAIMED IS:

1. A method of authenticating an electronic document, comprising the steps of:

signing the electronic document with a digital signature of a transfer agent;

appending a certificate to the electronic document by the transfer agent; and

validating the digital signature and certificate of the transfer agent.

2. The method of claim 1, wherein the certificate comprises an identity, public cryptographic key, and predetermined attributes of the transfer agent.

3. The method of claim 1, wherein the signing step comprises the steps of applying a hash function to the electronic document to determine a message digest and encrypting the message digest with a secret cryptographic key of the transfer agent.

4. The method of claim 3, wherein the step of validating the digital signature comprises the steps of decrypting the message digest with a public cryptographic key of the transfer agent, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest.

5. The method of claim 1, further comprising the step of applying a date stamp and a time stamp to the electronic document.

6. The method of claim 5, further comprising the step of signing the electronic document with a second digital signature after the digital signature has been validated.

7. An apparatus for authenticating an electronic document, comprising:

means for signing the electronic document with a digital signature of a transfer agent;

means for appending a certificate to the electronic document; and

means for validating the digital signature and certificate.

8. The apparatus of claim 7, wherein the certificate comprises an identity, public cryptographic key, and predetermined attributes of the transfer agent.

9. The apparatus of claim 7, wherein the signing means comprises means for applying a hash function to the electronic document to determine a message digest and means for encrypting the message digest with a secret cryptographic key of the transfer agent.

10. The apparatus of claim 9, wherein the validating means comprises means for decrypting the message digest with a public cryptographic key of the transfer agent, means for applying the hash function to the electronic document to determine a second message digest, and means for comparing the decrypted message digest to the second message digest.

11. The apparatus of claim 7, further comprising means for applying a date stamp and a time stamp to the electronic document.

12. The apparatus of claim 11, further comprising means for signing the electronic document with a second digital signature after the digital signature has been validated by the validating means.

13. An authentication system for electronic communication of documents and for ensuring integrity of transmitted documents and non-repudiation of the transmitted documents, comprising:

means for digitally encrypting a document;

means for certifying an identity of a transferor of the document;

means for generating a public key and a private key, at least one of the public key and the private key being used for digitally encrypting the document;

means for signing the document with a digital signature;

means for verifiably transmitting an encrypted, signed document; and

means for authenticating a transmitted, encrypted, signed document.

14. An electronic document storage and retrieval system that ensures authenticity of electronic documents stored in the system and transfers of electronic documents to authorized parties, comprising:

means for securely storing digitally encrypted electronic documents;

means for authenticating electronic documents retrieved from storage; and

means for verifying authority of a party requesting retrieval of an authenticated electronic document.

15. A method of authenticating electronically communicated documents that ensures integrity of the transmitted documents and non-repudiation of the transmitted documents, comprising the steps of:

digitally encrypting a document;

certifying an identity of a transferor of the document;

generating a public key and a private key, at least one of the public key and the private key being used for digitally encrypting the document;

signing the document with a digital signature;

verifiably transmitting an encrypted, signed document; and

authenticating a transmitted, encrypted, signed document.

16. The method of claim 15, wherein the certifying step includes a step of delivering a personal identification number and at least one of the public key and the private key to an originator of the document.

17. The method of claim 15, wherein the authenticating step comprises a step of including an integrity block and a date and time stamp in the transmitted, encrypted, signed document.

18. The authentication system of claim 13, further comprising means for sealing the encrypted, signed document, wherein the sealing means signs the encrypted, signed document with a second digital signature.

DAS

LIABILITY ALLOCATION USING PCM/CIA CARD AND DES

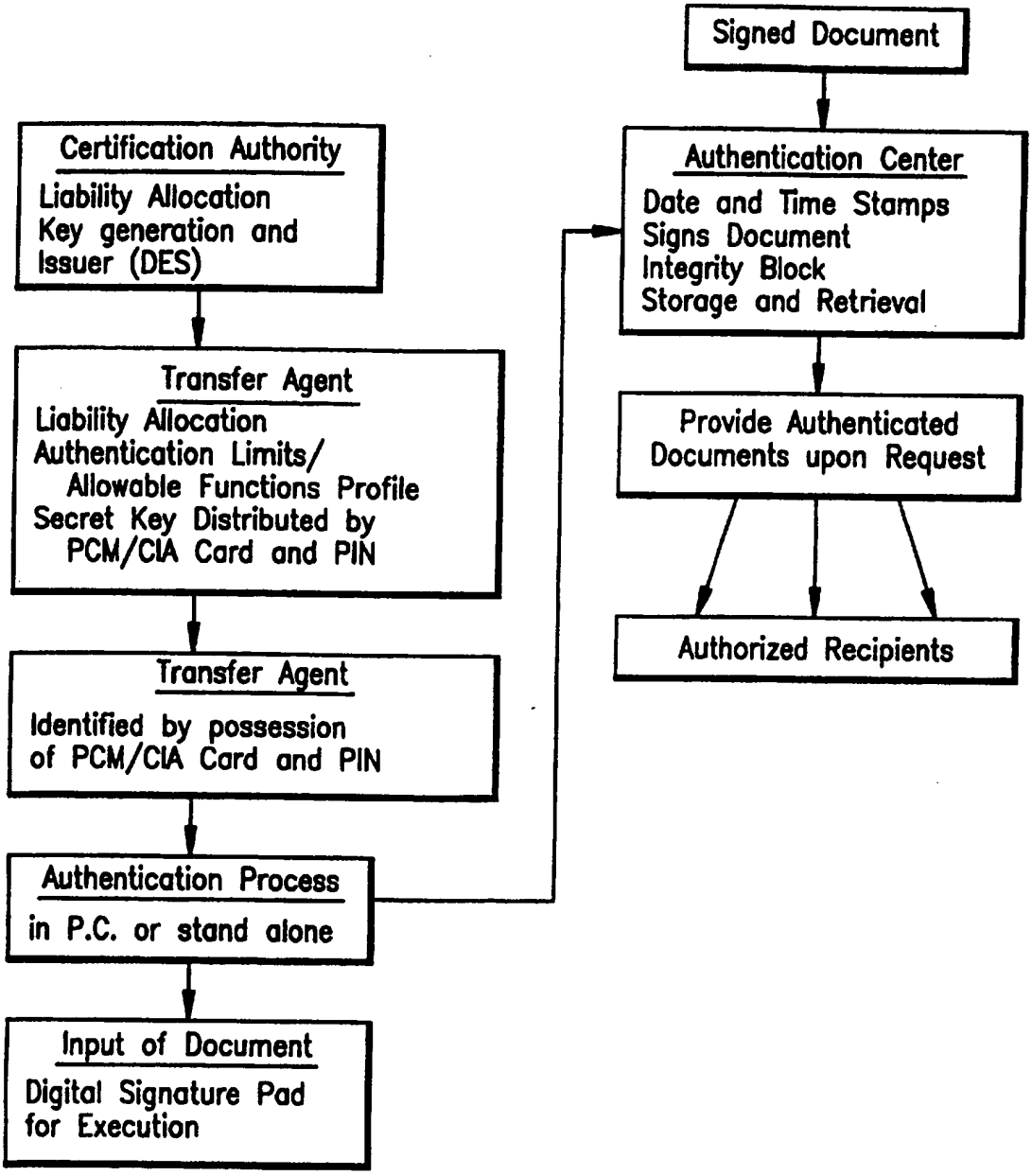


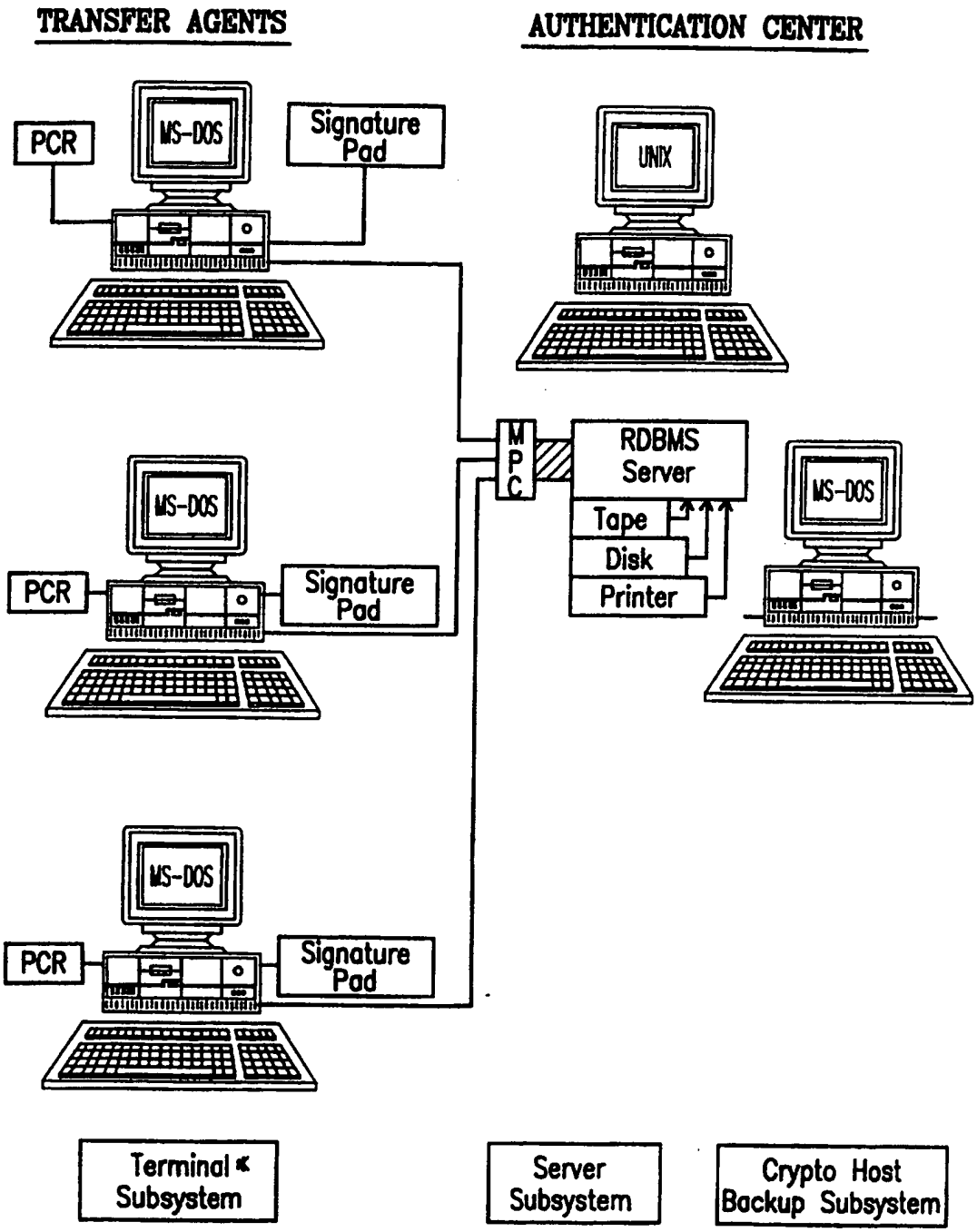
FIG. 1

PCCard	Terminal Software	DAS Services
Tamperproof cryptography *Provides cryptographic processing for:* PIN – Card activation & exposure of secret cryptographic materials Key exchange Key set Management of encryption, hash, and signature keys *Stores:* Card Characterization Information Certificates & Keys Software macros Attribute tables	Card Resource Manager Participates in Card authentication & activation Format data & performs I/O operations with Card Requests Card services	PIN validation Compute integrity value Sign Authenticate Signature Validate Integrity Time–stamp Encrypt/decrypt Manage keys Store Audit Trail & Liability Allocation

FIG. 2

DAS

DAS ARCHITECTURE

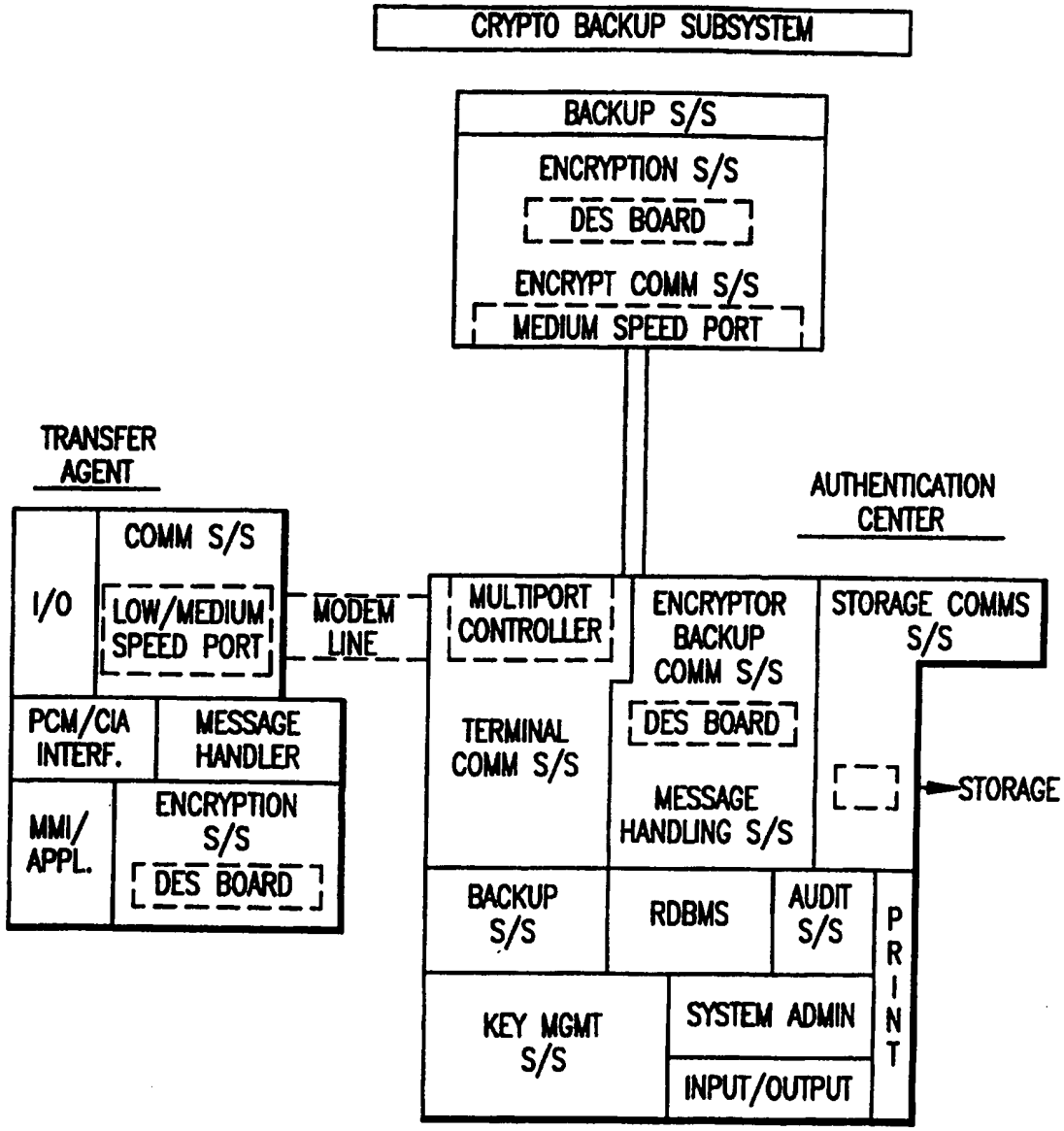


MPC – Multiport Controller
PCR – PCM/CIA Card Reader
* – 486/50 Laptop Computers may be utilized

FIG. 3

DAS

DAS FUNCTIONAL INTERRELATIONSHIP



TERMINAL SUBSYSTEM

Terminal: 486/50 PC
MS/DOS
Windows

Running Agent Application with transparent secure communications

SERVER SUBSYSTEM

Server: 486/50 System Pro
UNIX

Built Around Powerful multiuser RDBMS, supporting multiple terminal communications with complete audit and administration

Crypto Host: 486/50 PC
MS/DOS
Provides Encryption

FIG. 4

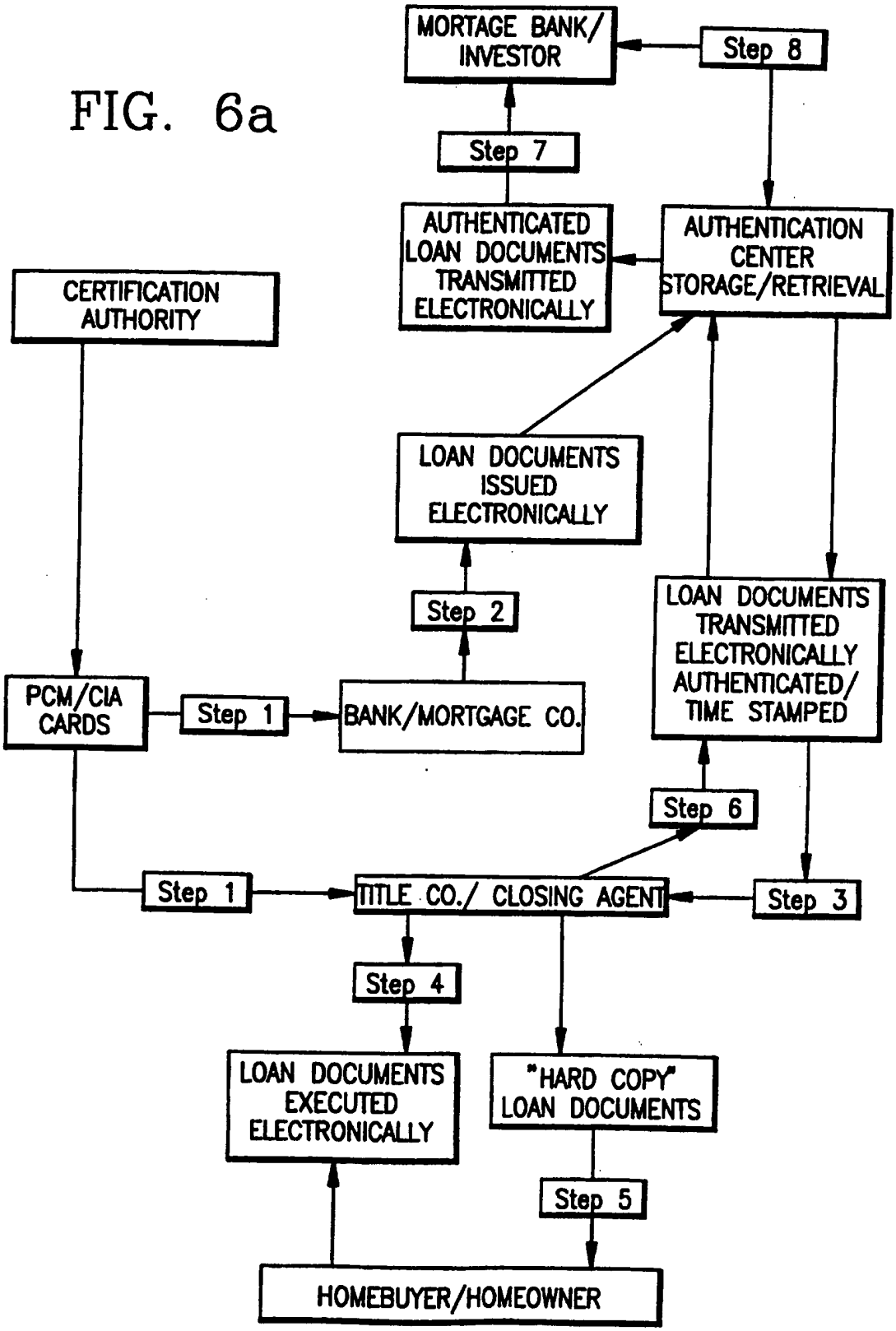
DAS

DAS CONTROL FUNCTIONS

CONTROL FUNCTIONS				
Confidentiality	Integrity	Non-repudiation (Signature)		Management Limits on User
		User	Authentication System	
Public key encryption of PIN and Keying Material	Digital Signature provides integrity protection	Digital sign. of user/ customer "signs" the transactions in a manner that cannot be repudiated.	Digital Sign. of AC "signs" the trans-actions in a manner that cannot be repudiated.	Limits for user profile stored on PCM/ CIA card
DES encryption of transactions			Integrity Block	PIN and PCM/ CIA card authentication to terminal and DAS system
			Date and Time stamp	

FIG. 5

FIG. 6a


DOCUMENT AUTHENTICATION SYSTEM LOAN TRANSACTION
MORTAGE BANK/ INVESTOR
Step 8
Step 7
AUTHENTICATED LOAN DOCUMENTS TRANSMITTED ELECTRONICALLY
AUTHENTICATION CENTER STORAGE/RETRIEVAL
CERTIFICATION AUTHORITY
LOAN DOCUMENTS ISSUED ELECTRONICALLY
Step 2
LOAN DOCUMENTS TRANSMITTED ELECTRONICALLY AUTHENTICATED/ TIME STAMPED
PCM/CIA CARDS
Step 1
BANK/MORTGAGE CO.
Step 6
Step 1
TITLE CO./ CLOSING AGENT
Step 3
Step 4
LOAN DOCUMENTS EXECUTED ELECTRONICALLY
"HARD COPY" LOAN DOCUMENTS
Step 5
HOMEBUYER/HOMEOWNER

DAS

DOCUMENT AUTHENTICATION SYSTEM
LOAN TRANSACTION

Chart Steps

Step 1. Complete Certification Authority code generation and card issuing to parties transferring the documents establishing legal evidence trail. Equip parties to transmit and receive documents

Step 2. Bank/Mortgage Co. loads and electronically transmits documents to Authentication Center which forwards to Title Co./Closing Agent

Step 3. Authentication Center transmits documents to Title Co./Closing Agent

Step 4. Title Co./Closing Agent has documents executed by digital signature by Homebuyer/Homeowner

Step 5. Title Co./Closing Agent provides Homeowner/Homebuyer with "Hard Copy" of signed documents

Step 6. Title Co./Closing Agent transmits documents to Authentication Center which dates and time stamps the executed documents and forwards documents to Bank/Mortgage Co.

. Whenever Bank/Mortgage Co. needs authentic documents, can retrieve on-line from Authentication Center storage

Step 7. Bank/Mortgage Co. directs authentic documents to be transferred by Authentication Authority to secondary market investor.

Step 8. Whenever investor needs authentic documents, can retrieve on-line from Authentication Center

FIG. 6b

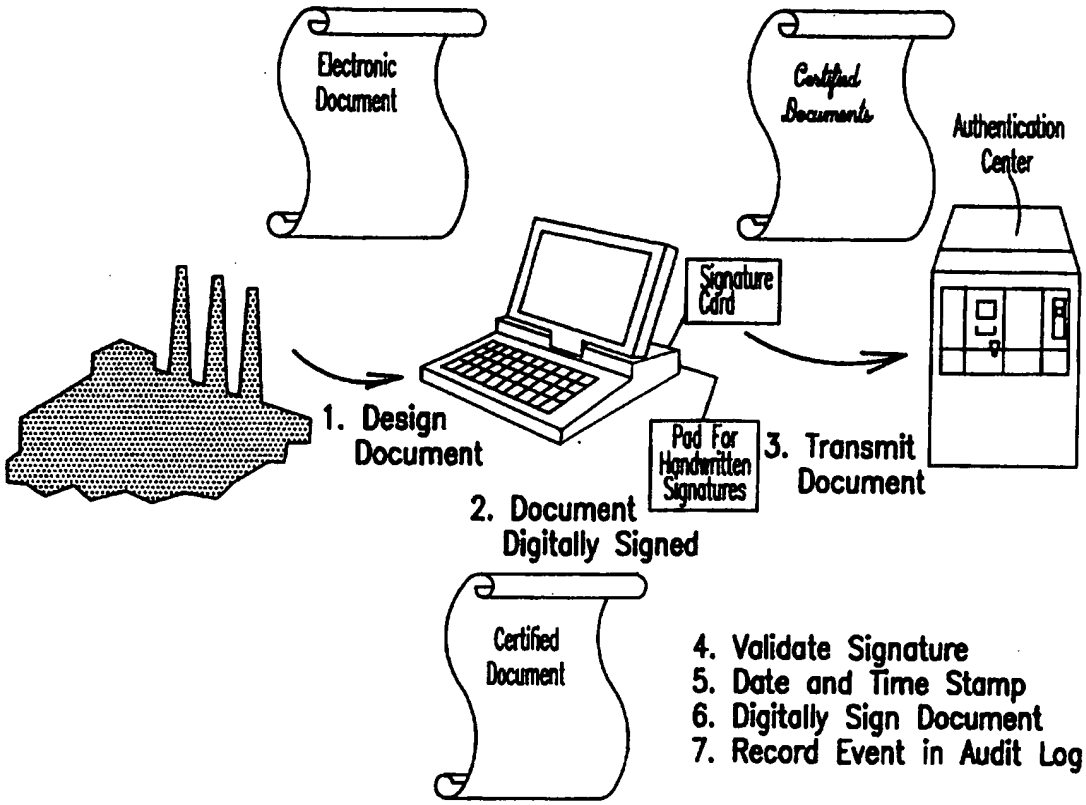

Electronic Document
Certified Documents
Authentication Center
Signature Card
1. Design Document
Pad For Handwritten Signatures
3. Transmit Document
2. Document Digitally Signed
Certified Document
4. Validate Signature
5. Date and Time Stamp
6. Digitally Sign Document
7. Record Event in Audit Log

FIG. 7

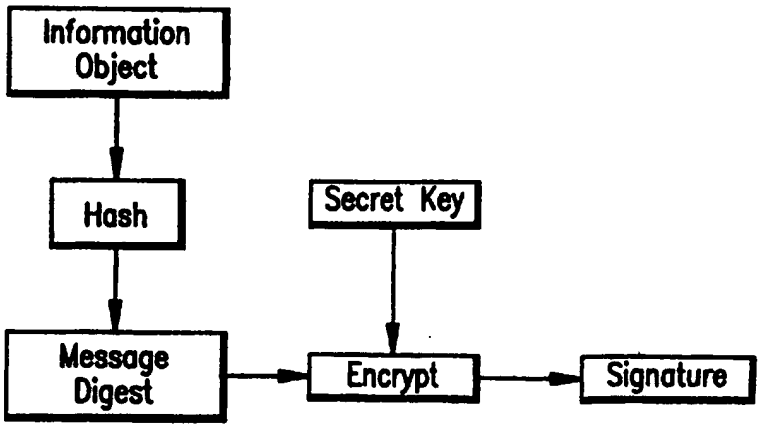

Information Object
Hash
Secret Key
Message Digest
Encrypt
Signature

FIG. 8

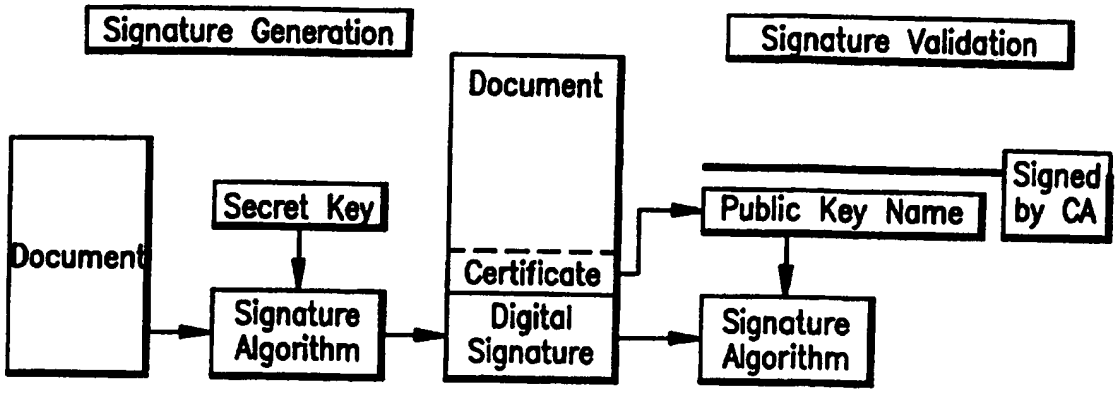

Signature Generation
Signature Validation
Document
Document
Secret Key
Signature Algorithm
Certificate
Digital Signature
Public Key Name
Signed by CA
Signature Algorithm

FIG. 9

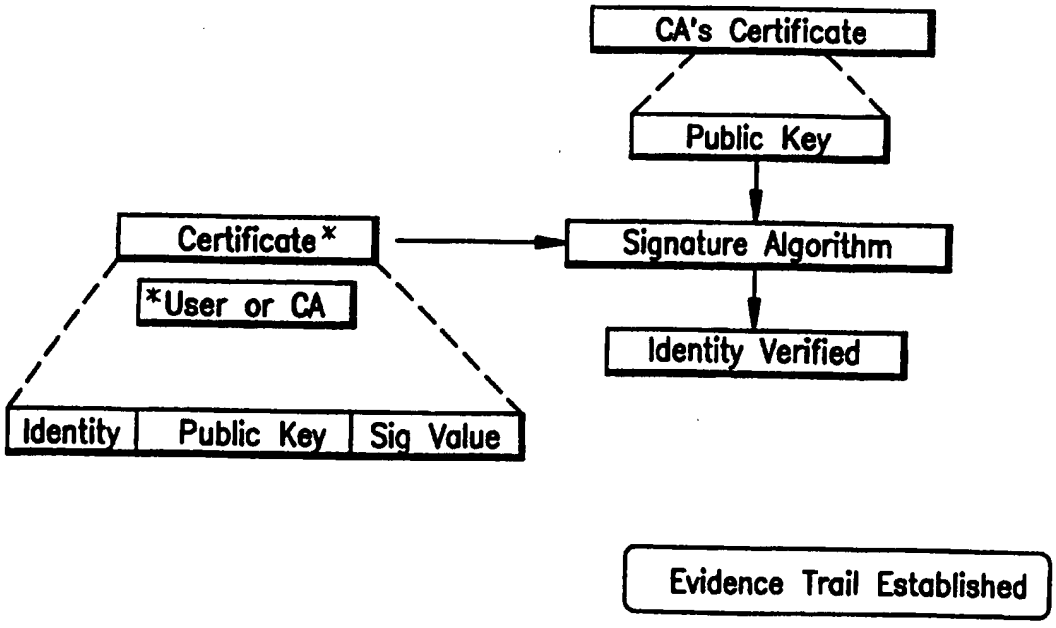

CA's Certificate
Public Key
Certificate*
*User or CA
Signature Algorithm
Identity Verified
Identity
Public Key
Sig Value
Evidence Trail Established

FIG. 11

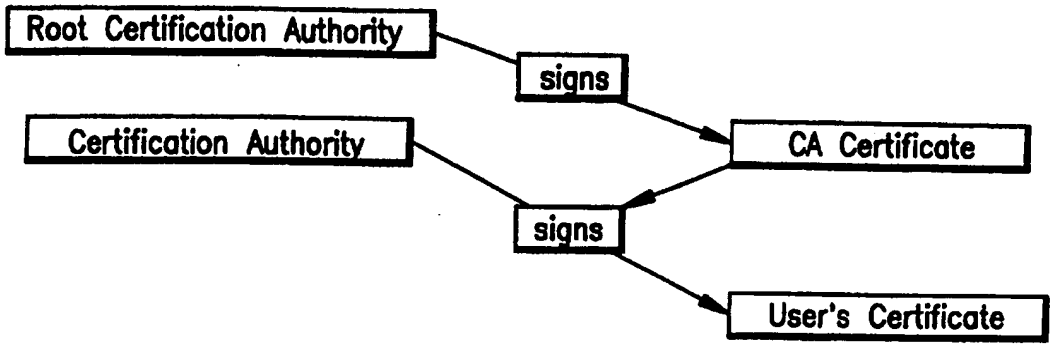


FIG. 12

CARICATURE OF X.509 CERTIFICATE
USER OR CERTIFICATION AUTHORITY

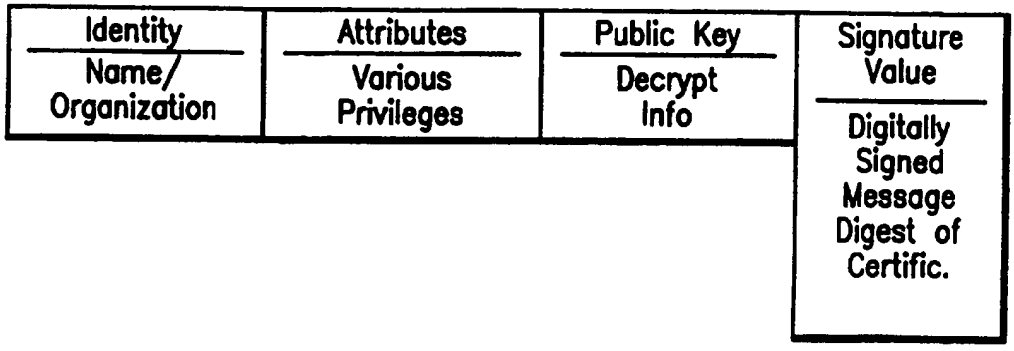


FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/14159

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/25

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25
380/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,231,668 (KRAVITZ) 27 July 1993, see Figs. 2-3.	1-18
Y	US, A, 5,371,794 (DIFFIE et al) 06 December 1994, see Figs. 46-56.	1-18
Y	US, A, 5,373,561 (HABER ET AL) 13 December 1994, see Figs. 1-2.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
12 DECEMBER 1996

Date of mailing of the international search report
03 MAR 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
SALVATORE CANGIALOSI
Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*